

New Protocols and Lower Bound for Quantum Secret Sharing with Graph States

Jérôme Javelle², Mehdi Mhalla^{1,2}, and Simon Perdrix^{1,2}

¹ CNRS

² LIG, Grenoble University, France

Abstract. We introduce a new family of quantum secret sharing protocols with limited quantum resources which extends the protocols proposed by Markham and Sanders [13] and Broadbent, Chouha, and Tapp [17]. Parametrized by a graph G and a subset of its vertices A , the protocol consists in: (i) encoding the quantum secret into the corresponding graph state by acting on the qubits in A ; (ii) use a classical encoding to ensure the existence of a threshold. These new protocols realize $((k, n))$ quantum secret sharing i.e., any set of at least k players among n can reconstruct the quantum secret, whereas any set of less than k players has no information about the secret. In the particular case where the secret is encoded on all the qubits, we explore the values of k for which there exists a graph such that the corresponding protocol realizes a $((k, n))$ secret sharing. We show that for any threshold $k \geq n - n^{0.68}$ there exists a graph allowing a $((k, n))$ protocol. On the other hand, we prove that for any $k < \frac{79}{156}n$ there is no graph G allowing a $((k, n))$ protocol. As a consequence there exists n_0 such that the protocols introduced by Markham and Sanders in [13] admit no threshold k when the secret is encoded on all the qubits and $n > n_0$.

Keywords: Quantum Cryptography, Secret Sharing, Graphs, Graph States.

1 Introduction

Secret sharing schemes were independently introduced by Shamir [16] and Blakley [1] and extended to the quantum case by Hillery [9] and Gottesman [3,6].

A $((k, n))$ quantum secret sharing [9,3,6] is a protocol by which a dealer distributes shares of a quantum secret to n players such that any subset of at least k players can reconstruct the secret by combining their shares, while any set of less than k players cannot have any information about the secret. It is assumed that the secret is an arbitrary one-qubit state, that the dealer has only one copy of the secret he wants to share and that the players can communicate together using classical and quantum channels.

A direct consequence of the no-cloning theorem [19] is that no $((k, n))$ quantum secret sharing protocol can exist when $k \leq \frac{n}{2}$ – otherwise two distinct sets

of players can reconstruct the secret implying a cloning of quantum secret. On the other hand, for any $k > \frac{n}{2}$ a $((k, n))$ protocol has been introduced in [6] in such a way that the dimension of each share is proportional to the number of players.

The unbounded size of the share is a strong limitation of the protocol, as a consequence several schemes of quantum secret sharing using a bounded amount of resources for each player have been introduced [13,17,12]. In particular, in [13] a quantum secret sharing scheme using graph states is presented where each player receives a single qubit. At the forefront in terms of implementation, the graph states has emerged as a powerful and elegant family of entangled state [8,18].

Only few threshold quantum secret sharing schemes have been proved in the literature to be achievable using graph states: $((3, 5))$ can be done using a C_5 graph (cycle with 5 vertices), and for any n , an $((n, n))$ protocol using the complete graph can be done, up to some constraints on the quantum secret [13]. Independently [17] introduced an $((n, n))$ protocol for any n . This protocol is based on the GHZ state [7] which is locally equivalent to a complete graph state [8]. The technique which consists in mixing the quantum secret before to encode it into a larger state is also used in [14] in such a way that some players have a classical share but no quantum share.

We introduce a new family of secret sharing protocols using graph states. Like in [13] the quantum secret is encoded into a graph state shared between the players, but in order to obtain threshold protocols, an additional round is added to the protocol. This round consists in mixing the quantum secret using a one-time pad scheme which classical key is then shared between the players using a classical secret sharing protocol. This technique extends the one presented in [17] in which the secret is partially mixed and then shared using a fixed quantum state, namely the GHZ state which is equivalent to the complete graph state. Independently, a hybrid classical-quantum construction of QSS has been recently proposed in [5] where they optimize the quantum communication complexity when the size of the secret is greater than the number of players.

The family of protocols we introduce in the present paper is parametrised by a pair (G, A) where G is a graph and A is a non empty set of vertices of the graph. We explore the possible values of k for which there exists a pair (G, A) leading to a $((k, n))$ protocol. Our main results are: first, we introduce a family of graphs which can realise any $((k, n))$ protocol when $k > n - n^{0.68}$. This result proves that graph states secret sharing can be used not only for $((n, n))$ protocols, but also for any threshold larger than $n - n^{0.68}$. The second main result of the paper is the proof that there is no graph G such that $(G, V(G))$ realizes a $((k, n))$ protocols when $k < \frac{79}{156}n$. Notice that this lower bound also applies in

the protocol introduced by Markham and Sanders. Moreover, it suggests that secret sharing protocols with a threshold closed to half of the players cannot be achieved with shares of bounded size.

Section 2 is dedicated to the description of the various secret sharing protocols based on graph states: section 2.1 describes the protocol cQSS introduced in [13] for sharing a classical secret, while section 2.2 describes its extension to a quantum secret qQSS. We prove that the sufficient combinatorial conditions for accessibility and privacy introduced in [11] for these protocols are actually necessary. These graphical characterisations are key ingredients for proving the main results of this paper. In section 2.3 the new family of protocols qQSS* is introduced. In section 3 we prove that for any $k > n - n^{0.68}$ there exists a qQSS* protocol which realises a $((k, n))$ secret sharing. Finally, in section 4, we prove the following lower bound: for any $k < \frac{79}{156}n$ there is no graph G such that $(G, V(G))$ realises a $((k, n))$ qQSS* scheme. A preliminary version of this work has been presented at [10].

2 Graph state secret sharing

2.1 Sharing a classical secret using a graph state

For a given graph G on n vertices v_1, \dots, v_n , the corresponding graph state $|G\rangle$ is a n -qubit quantum state defined as

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q(x)} |x\rangle$$

where $q(x)$ is the number of edges in the induced subgraph $G_x = (\{v_i \in V(G) \mid x_i = 1\}, \{(v_i, v_j) \in E(G) \mid x_i = x_j = 1\})$.

Graph states have the following fundamental fixpoint property: given a graph G , for any vertex $u \in V(G)$,

$$X_u Z_{N(u)} |G\rangle = |G\rangle$$

where $N(u)$ is the neighborhood of u in G , $X = |x\rangle \mapsto |\bar{x}\rangle$, $Z = |x\rangle \mapsto (-1)^x |x\rangle$ are one-qubit Pauli operators and $Z_A = \bigotimes_{u \in A} Z_u$ is a Pauli operator acting on the qubits in A . As a consequence, for any subset $D \subseteq V(G)$ of vertices, $\bigotimes_{u \in D} X_u Z_{N(u)} |G\rangle = |G\rangle$. Since X and Z anti-commutes and $Z^2 = X^2 = I$,

$$(-1)^{|D \cap \text{Odd}(D)|} X_D Z_{\text{Odd}(D)} |G\rangle = \bigotimes_{u \in D} X_u Z_{N(u)} |G\rangle = |G\rangle$$

where $\text{Odd}(D) := \{v \in V(G) \text{ s.t. } |N(v) \cap D| = 1 \bmod 2\}$ is the odd neighborhood of D .

We present a family of quantum protocols for sharing a classical secret (cQSS) parametrized by a graph G and a non empty subset A of the vertices of the graph. This family of protocols has been introduced in [13]. Obviously, sharing a classical bit can be done using a classical scheme, like [16], instead of using a quantum state. However, the study of the cQSS protocols, and in particular the characterisation of accessibility and privacy (see corollary 1) are essential for the next sections where the sharing of a quantum secret is considered.

Suppose a dealer wants to share a classical secret $s \in \{0, 1\}$ between $n = |V(G)|$ players. The dealer prepares the state $|G_s\rangle = Z_A^s |G\rangle$ where Z_A^0 is the identity and Z_A^1 consists in applying the Pauli operator Z on each qubit of A . The dealer sends each player i the qubit q_i of $|G_s\rangle$. Regarding the reconstruction of the secret, a set B of players can recover the secret if and only if $\text{tr}(\rho_B(0)\rho_B(1)) = 0$, i.e. if the set of players can distinguish perfectly between the two states $\rho_B(0)$ and $\rho_B(1)$, where $\rho_B(s) = \text{tr}_{V \setminus B}(|G_s\rangle \langle G_s|)$ is the state of the subsystem of the players in B . On the other hand, a set B of players has no information about the secret if and only if $\rho(0)$ and $\rho(1)$ are indistinguishable, i.e. $\rho(0) = \rho(1)$.

Sufficient graphical conditions for accessibility and privacy have been proved in [11]:

Lemma 1 ([11]). *Given a cQSS protocol (G, A) , for any $B \subseteq V(G)$,*
– *If $\exists D \subseteq B$ s.t. $D \cup \text{Odd}(D) \subseteq B$ and $|D \cap A| \equiv 1 \pmod{2}$ then B can access the secret.*
– *If $\exists C \subseteq \overline{B} = V(G) \setminus B$ s.t. $\text{Odd}(C) \cap B = A \cap B$ then B has no information about the secret.*

According to the previous lemma, for a given set of players $B \subseteq V(G)$, if $\exists D \subseteq B$ s.t. $D \cup \text{Odd}(D) \subseteq B$ and $|D \cap A| \equiv 1 \pmod{2}$ then B can access the secret. More precisely, the players in B perform a measurement of their qubits according to the observable $(-1)^{|D \cap \text{Odd}(D)|} X_D Z_{\text{Odd}(D)}$. This measurement produces a classical outcomes $s \in \{0, 1\}$ which is the reconstructed secret [11].

We prove that the sufficient graphical conditions are actually necessary conditions, and that any set of players is either able to access the secret or has no information about the secret.

Lemma 2. *Given a graph G and $A \subseteq V(B)$, for any $B \subseteq V(G)$, B satisfies exactly one of the two properties:*

- i. $\exists D \subseteq B, D \cup \text{Odd}(D) \subseteq B \wedge |D \cap A| \equiv 1 \pmod{2}$
- ii. $\exists C \subseteq V \setminus B, \text{Odd}(C) \cap B = A \cap B$

Proof. For a given $B \subseteq V(G)$, let $\Gamma_{B, \overline{B}}$ be the cut matrix induced by B , i.e. the sub-matrix of the adjacency matrix Γ of G such that the columns

of $\Gamma_{B,\overline{B}}$ correspond to the vertices in B and its rows to the vertices in \overline{B} . $\Gamma_{B,\overline{B}}$ is the matrix representation of the linear function which maps every $X \subseteq B$ to $\Gamma_{B,\overline{B}}.X = \text{Odd}(X) \cap \overline{B}$, where the set X is identified with its characteristic column vector. Similarly, $\forall Y \subseteq \overline{B}$, $\Gamma_{\overline{B},B}.Y = \text{Odd}(Y) \cap B$ where $\Gamma_{\overline{B},B} = \Gamma_{B,\overline{B}}^T$ since Γ is symmetric. Moreover, notice that for any set $X, Y \subseteq V(G)$, $|X \cap Y| \bmod 2$ is given by the matrix product $Y^T.X$ where again sets are identified with their column vector representation. Equation (i) is satisfied iff $\exists D$ s.t. $\left(\frac{(A \cap B)^T}{\Gamma_{B,\overline{B}}}\right).D = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ which is equivalent to $\text{rank}\left(\frac{(A \cap B)^T}{\Gamma_{B,\overline{B}}}\right) = \text{rank}\left(\frac{(A \cap B)^T}{\Gamma_{B,\overline{B}}} \middle| \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \text{rank}\left(\frac{0}{\Gamma_{B,\overline{B}}} \middle| \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \text{rank}(\Gamma_{B,\overline{B}}) + 1$. Thus (i) is true iff $R(B) = 1$ where $R(B) := \text{rank}\left(\frac{(A \cap B)^T}{\Gamma_{B,\overline{B}}}\right) - \text{rank}(\Gamma_{B,\overline{B}})$. Similarly equation (ii) is satisfied iff $\exists C$ s.t. $\Gamma_{\overline{B},B}.C = A \cap B$ iff $\text{rank}(\Gamma_{\overline{B},B}|A \cap B) = \text{rank}(\Gamma_{\overline{B},B})$. Thus (ii) is true iff $R(B) = 0$. Since for any $B \subseteq V(G)$, $R(B) \in \{0, 1\}$ it comes that either (i) is true or (ii) is true. \square

Corollary 1. *Given a cQSS protocol (G, A) , for any $B \subseteq V(G)$,*
 $\exists D \subseteq B, D \cup \text{Odd}(D) \subseteq B \wedge |D \cap A| = 1 \bmod 2 \iff B \text{ can access the secret.}$
 $\exists C \subseteq V \setminus B, \text{Odd}(C) \cap B = A \cap B \iff B \text{ has no information about the secret.}$

2.2 Sharing a quantum secret

Following [13], the cQSS protocols are extended to qQSS schemes for sharing a quantum secret $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Given a graph G and A a non empty subset of vertices, the dealer prepares the quantum state $|G_\phi\rangle = \alpha|G_0\rangle + \beta|G_1\rangle$. Notice that the transformation $|\phi\rangle \mapsto |G_\phi\rangle$ is a valid quantum evolution – i.e. an isometry – whenever $|G_0\rangle$ is orthogonal to $|G_1\rangle$ which is guaranteed by $A \neq \emptyset$. Then, the dealer sends each player i the qubit q_i of $|G_\phi\rangle$. Regarding the reconstruction of the secret, it has been proved in [13], that a set B of players can recover the quantum state $|\phi\rangle$ if and only if B can reconstruct a classical secret in the two protocols $cQSS(G, A)$ and $cQSS(G \Delta A, A)$, where $G \Delta A = (V(G), E(G) \Delta (A \times A))$ and $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$ is the symmetric difference. In other words $G \Delta A$ is obtained by complementing the edges of G incident to two vertices in A . We introduce an alternative characterisation of q-accessibility (ability to reconstruct a quantum secret) which does not involved the complemented graph $G \Delta A$:

Lemma 3. *Given a qQSS protocol (G, A) , a set B of players can reconstruct the quantum secret if and only if, in the protocol $cQSS(G, A)$, B can reconstruct the classical secret and $\overline{B} = V(G) \setminus B$ cannot.*

Proof. First notice that for any X , if $|X \cap A| = 1 \bmod 2$ then $Odd_{G\Delta A}(X) = Odd_G(X)\Delta A$. Thus for any X, Y , if $|X \cap A| = 1 \bmod 2$, $Odd_{G\Delta A}(X) \cap Y = \emptyset \iff (Odd_G(X)\Delta A) \cap Y = \emptyset \iff (Odd_G(X) \cap Y)\Delta(A \cap Y) = \emptyset \iff Odd_G(X) \cap Y = A \cap Y$.

(\Rightarrow) Assume that B can reconstruct the quantum secret, so B can reconstruct the classical secret in $G\Delta A$. Thus $\exists D \subseteq B$ s.t. $Odd_{G\Delta A}(D) \cap \overline{B} = \emptyset$. According to the previous remark, it implies that $Odd_G(D) \cap \overline{B} = A \cap \overline{B}$, so \overline{B} cannot reconstruct the secret.

(\Leftarrow) Assume \overline{B} cannot recover the classical secret and B can. So $\exists C \subseteq B$ s.t. $Odd_G(C) \cap B = A \cap B$. If $|C \cap A|$ is even, let $C' := C\Delta D$ where $|D \cap A|$ is odd and $Odd_G(D) \cap B = \emptyset$. Such a set D exists since B can reconstruct the classical secret in G . If $|C \cap A|$ is odd, then let $C' := C$. In both cases, $|C' \cap A| = 1 \bmod 2$ and $Odd_G(C') \cap B = A \cap B$, so according to the previous remark, $Odd_{G\Delta A}(C') \cap B = \emptyset$, as a consequence B can access the classical secret in $G\Delta A$. \square

In any pure quantum secret sharing protocol a set of players can reconstruct a quantum secret if and only if its complement set of players has no information about the secret (see [6]). As a consequence:

Corollary 2. *Given a qQSS protocol (G, A) , a set B of players has no information about the quantum secret if and only if, in the protocol cQSS (G, A) , \overline{B} can reconstruct the classical secret and B cannot.*

Sets of players that can reconstruct the secret and those who have no information about the secret admit simple graphical characterisation thanks to the simple reduction to the classical case. However, contrary to the cQSS case, there is a third kind of set players, those who can have some information about the secret but not enough to reconstruct the secret perfectly. For instance for any $n > 1$ consider the qQSS protocol $(K_n, \{v_1, \dots, v_n\})$ where K_n is the complete graph on the n vertices v_1, \dots, v_n . For any set B of vertices s.t. $B \neq \emptyset$ and $\overline{B} \neq \emptyset$, both B and \overline{B} cannot reconstruct a classical secret in the corresponding cQSS protocol, so B cannot reconstruct the quantum secret perfectly but has some information about the secret.

Corollary 3. *The qQSS protocols (G, A) and $(G\Delta A, A)$ have the same accessing structures – i.e. a set of players can access the secret in (G, A) iff it can access the secret in $(G\Delta A, A)$. In particular, the protocols $(G, V(G))$ and $(\overline{G}, V(G))$ have the same accessing sets.*

2.3 Threshold schemes

For any qQSS protocol (G, A) , the accessing structures can be characterized. For secret sharing protocols, this is often interesting to focus on threshold protocols, i.e. protocols such that there exists an integer k such that any set of least k players can reconstruct the secret, whereas any set of at most $k - 1$ players have no information about the secret. Such threshold protocols are denoted $((k, n))$. In [6], it has been proved that if the dealer is sending a pure quantum state to the players, like in the qQSS protocols, then the threshold, if it exists, should be equal to $\frac{n+1}{2}$ where n is the number of players. This property which is derived from the no-cloning theorem, is very restrictive. It turns out that there is a unique threshold for which a qQSS protocol is known. This protocol is $(C_5, \{v_1, \dots, v_5\})$ where C_5 is the cycle graph on 5 vertices. The threshold for this protocol is 3. In section 4, we prove that under the constraint that $A = V(G)$, there is no threshold qQSS protocol for $n > 79$.

However, in general a qQSS protocol corresponds to a ramp secret sharing scheme [15] where any set of players smaller than $n - k$ cannot access the information and any set greater than k can. In this section we show how these ramp schemes can be turned into threshold schemes by adding a classical secret sharing round.

Theorem 1. *Given a graph G over n vertices, a non empty subset of vertices A , and an integer k , such that $\forall B \subseteq V(G)$ with $|B| = k$, $\exists C_B, D_B \subseteq B$ satisfying $|D_B \cap A| = 1 \pmod 2$, $\text{Odd}(D_B) \subseteq B$, and $\text{Odd}(C_B) \cap \overline{B} = A \cap \overline{B}$, it exists an $((k + c, n + c))$ quantum secret sharing protocol for any $c \geq 0$ in which the dealer sends one qubit to n players and uses a $(k + c)$ -threshold classical secret sharing scheme on the $n + c$ players.*

The rest of the section is dedicated to define a family of protocols called $qQSS^*$ satisfying the theorem.

Inspired by the work of Broadbent, Chouha and Tapp [17], we extend the qQSS scheme adding a classical reconstruction part. In [17], a family of unanimity – i.e. the threshold is the number of players – quantum secret sharing protocols have been introduced. They use a GHZ state which equivalent to the graph state $|K_n\rangle$ where K_n is the complete graph on n vertices. We extend this construction to any graph, using also a more general initial encryption corresponding to a quantum one-time pad of the quantum secret.

Quantum secret sharing with graph states and classical reconstruction ($qQSS^*$). Given a graph G , a non empty subset of players A , and an integer k , such that $\forall B \subseteq V(G)$ if $|B| \geq k$ then $\exists C_B, D_B \subseteq B$ satisfying $|D_B \cap A| = 1 \pmod 2$, $\text{Odd}(D_B) \subseteq B$, and $\text{Odd}(C_B) \cap \overline{B} = A \cap \overline{B}$. Suppose the dealer wishes to share the quantum secret $|\phi\rangle = \alpha|0\rangle + |1\rangle$.

- **Encryption.** The dealer chooses uniformly at random $b_x, b_z \in \{0, 1\}$. and apply $X^{b_x} Z^{b_z}$ on $|\phi\rangle$. The resulting state is $|\phi'\rangle = \alpha |b_x\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle$.
- **Graph state embedding.** The dealer embeds $|\phi'\rangle$ to the n -qubit state $\alpha |G_{b_x}\rangle + \beta(-1)^{b_z} |G_{\overline{b_x}}\rangle$.
- **Distribution.** The dealer sends each player i the qubit q_i . Moreover using a classical secret sharing scheme with a threshold k , the dealer shares the bits b_x, b_z .
- **Reconstruction.** The reconstruction of the secret for a set B of players s.t. $|B| \geq k$ is in 3 steps: first the set D_B is used to add an ancillary qubit and put the overall system in an appropriate state; then C_B is used to disentangled the ancillary qubit from the rest of the system; finally the classical bits b_x and b_z are used to recover the secret:
 - (a) The players in B applies on their qubits the isometry $U_{D_B} := |0\rangle \otimes P_0 + |1\rangle \otimes P_1$ where P_i are the projectors associated with observable $\mathcal{O}_{D_B} = (-1)^{|D_B \cap \text{Odd}(D_B)|} X_{D_B} Z_{\text{Odd}(D_B)}$, i.e. $P_i := \frac{I + (-1)^i \mathcal{O}_{D_B}}{2}$. The resulting state is $\alpha |b_x\rangle \otimes |G_{b_x}\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle \otimes |G_{\overline{b_x}}\rangle$.
 - (b) The players in B apply the controlled unitary map $A_{V_{C_B}} = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes V_{C_B}$, where $V_C := (-1)^{|C \cap \text{Odd}(C)|} X_C Z_{\text{Odd}(C) \Delta A}$. The resulting state is $\alpha |b_x\rangle \otimes |G\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle \otimes |G\rangle = (\alpha |b_x\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle) \otimes |G\rangle$.
 - (c) Thanks to the classical secret sharing scheme, the players in B recover the bits b_x and b_z . They apply X^{b_x} and then Z^{b_z} for reconstructing the quantum secret $\alpha |0\rangle + \beta |1\rangle$ on the ancillary qubit.

Note that this reconstruction method can be used for the qQSS protocols defined in [11] and for which the reconstruction part was not explicitly defined.

Lemma 4. *A qQSS* protocol (G, A, k) is a $((k, |V(G)|))$ secret sharing protocol if for any $B \subseteq V(G)$ s.t. $|B| \geq k$, B can reconstruct the secret in qQSS(G, A).*

Proof. The classical encoding ensures that any set of size smaller than k cannot access to the secret. \mathcal{O}_{D_B} is acting on the qubits $D_B \cap \text{Odd}(D_B) \subseteq B$. Moreover $P_i |G_s\rangle = |G_s\rangle$ if $i = s$ and 0 otherwise, so the application of the isometry U_{D_B} produce the state $\alpha |b_x\rangle \otimes |G_{b_x}\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle \otimes |G_{\overline{b_x}}\rangle$. Regarding step b of the reconstruction, since $\text{Odd}(C) \cap \overline{B} = A \cap \overline{B}$, $C \cup \text{Odd}(C) \Delta A \subseteq B$ V_C is acting on the qubits in B . Moreover V_C produces the states $(\alpha |b_x\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle) \otimes |G\rangle$. Finally the classical secret scheme guarantees that the players in B have access to b_x and b_z so that they reconstruct the secret. \square

Proof of Theorem 1. The correctness of the qQSS* protocol implies that given a graph G over n vertices, a non empty subset of vertices A , and an

integer k , such that $\forall B \subseteq V(G)$ with $|B| = k$, $\exists C_B, D_B \subseteq B$ satisfying $|D_B \cap A| = 1 \pmod{2}$, $\text{Odd}(D_B) \subseteq B$, and $\text{Odd}(C_B) \cap \overline{B} = A \cap \overline{B}$, it exists a $((k, n))$ protocol. In order to finish the proof of Theorem 1 this protocol is turned into a $((k + c, n + c))$ protocol for any $c \geq 0$ the qQSS* protocol is modified as follows, following the technique used in [14]. During the distribution stage, the dealer shares b_x and b_z with all the $n + c$ players with a threshold $k + c$, but sends a qubit of the graph state to only n players chosen at random among the $n + c$ players. During the reconstruction, a set of $k + c$ players must contain at least k players having a qubit. This set use the reconstruction steps a and b and then the last step c is done by all the $k + c$ players. \square

In the following we focus on the particular case where $A = V(G)$.

3 Building $((n - n^{0.68}, n))$ -qQSS* Protocols

We give a construction of an infinite family of quantum secret sharing schemes $((k, n))$ where $k = n - n^{\frac{\log(3)}{\log(5)}} < n - n^{0.68}$. This construction can be defined recursively from cycle over 5 vertices (C_5) which has been used in Markham and Sanders [13] to build a $((3, 5))$ quantum secret sharing protocol.

We define a composition law $*$ between two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ as follows:

Definition 1. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs. The lexicographic product $*$ of two graphs G_1 and G_2 is defined as follows: $V(G_1 * G_2) := V_1 \times V_2$ and $E(G_1 * G_2) := \{((u_1, u_2), (v_1, v_2)) \mid (u_1, v_1) \in E_1 \text{ or } (u_1 = v_1 \wedge (u_2, v_2) \in E_2)\}$.

In other terms, the graph G is a graph G_1 which vertices are replaced by copies of the graph G_2 , and which edges are replaced by complete bipartitions between two copies of the graph G_2 (Figure 1).

Lemma 5. For any graphs G_1 and G_2 , $\overline{G_1 * G_2} = \overline{G_1} * \overline{G_2}$

Proof. It is easy to see that $V(\overline{G_1 * G_2}) = V(\overline{G_1} * \overline{G_2})$. We want to show that $E(\overline{G_1 * G_2}) = E(\overline{G_1} * \overline{G_2})$.

Consider an edge $((u_1, u_2), (v_1, v_2)) \in E(\overline{G_1 * G_2})$. If $u_1 = v_1$ then $(u_2, v_2) \notin E_2$. Otherwise $(u_1, v_1) \notin E_1$. Thus $(u_1, v_1) \in \overline{E_1}$ or $(u_1 = v_1 \text{ and } (u_2, v_2) \in \overline{E_2})$ which means, by definition, that $((u_1, u_2), (v_1, v_2)) \in E(\overline{G_1} * \overline{G_2})$. Therefore, $E(\overline{G_1 * G_2}) \subseteq E(\overline{G_1} * \overline{G_2})$.

Furthemore $|E(\overline{G_1} * \overline{G_2})| = n_1|E(\overline{G_2})| + n_2^2|E(\overline{G_1})|$ where $n_1 = |V_1|$ and $n_2 = |V_2|$. Thus $|E(\overline{G_1} * \overline{G_2})| = n_1n_2(n_1n_2 - 1)/2 - (n_1E(G_2) + n_2^2E(G_1)) = |E(\overline{G_1 * G_2})|$. Therefore $E(\overline{G_1 * G_2}) = E(\overline{G_1} * \overline{G_2})$. \square

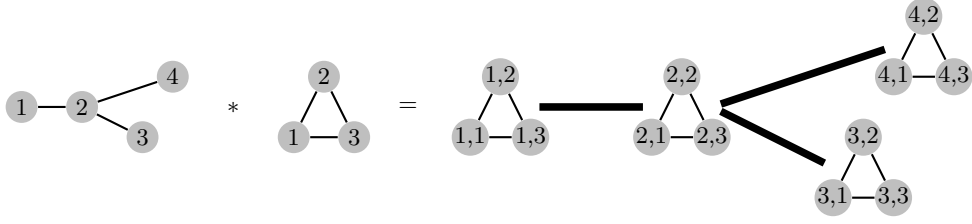


Fig. 1. Graphical explanation of the composition law $*$ between two graphs. A thick line represents a complete bipartition between two triangle graphs.

Lemma 6. Let G_1, G_2 be two graphs such that $G_1 = (V_1, E_1)$ realizes an $((k_1, n_1))$ $qQSS^*$ protocol and $G_2 = (V_2, E_2)$ realizes a $((k_2, n_2))$ $qQSS^*$ protocol. The graph $G = G_1 * G_2 = (V, E)$ realizes an $((k, n))$ $qQSS^*$ protocol where

$$\begin{cases} n = n_1 n_2 \\ k = n_1 n_2 - (n_1 - k_1 + 1)(n_2 - k_2 + 1) + 1 \end{cases}$$

Proof. First we show that if $G_1 = (V_1, E_1)$ realizes an $((k_1, n_1))$ $qQSS^*$ protocol and $G_2 = (V_2, E_2)$ realizes an $((k_2, n_2))$ $qQSS^*$, then, in the graph $G = G_1 * G_2 = (V, E)$, for any set $B \subseteq V$ of size k (with $k = n_1 n_2 - (n_1 - k_1 + 1)(n_2 - k_2 + 1) + 1$) it exists a set D_B such that $|D_B| = 1 \pmod 2$, $Odd(D_B) \subseteq B$.

For any set $B \subseteq V$ and any vertex $v_1 \in V$, let $B_2(v_1) = \{v_2 \in V_2 \text{ s.t. } (v_1, v_2) \in B\}$ and $B_1 = \{v_1 \in V_1 \text{ s.t. } |B_2(v_1)| \geq k_2\}$.

We claim that for all set $B \subseteq V$ of size $|B| = k$, the size of the set B_1 verifies $|B_1| \geq k_1$.

By contradiction, notice that $B = \bigcup_{v_2 \in B_2(v_1), v_1 \in V_1} \{(v_1, v_2)\}$. Therefore: $|B| = |V| - \sum_{v_1 \in B_1} |V_2 \setminus B_2(v_1)| - \sum_{v_1 \in V_1 \setminus B_1} |V_2 \setminus B_2(v_1)|$. Thus $|B| \leq n_1 n_2 - |V_1 \setminus B_1|(n_2 - k_2 + 1) \leq k - 1$ if $|B_1| \leq k_1$.

Now we consider any set $B \subseteq V$ of size $|B| = k$. As $|B_1| \geq k_1$, it exists a set $D_1 \subseteq B_1$ with $|D_1| = 1 \pmod 2$ and $D_1 \cup Odd(D_1) \subseteq B_1$.

Furthermore for any $v_1 \in B_1$, $|B_2(v_1)| \geq k_2$ and thus there exists $D_2(v_1) \subseteq B_2(v_1)$ with $|D_2(v_1)| = 1 \pmod 2$ and $D_2(v_1) \cup Odd(D_2(v_1)) \subseteq B_2(v_1)$ and there exist $C_2(v_1) \subseteq B_2(v_1)$ with $V_2 \setminus B_2(v_1) \subseteq Odd(C_2(v_1))$.

Let $C_2^0(v_1) = C_2(v_1)$ if $|C_2(v_1)| = 0 \pmod 2$ and $C_2^0(v_1) \Delta D_2(v_1)$ otherwise, and let $C_2^1(v_1) = C_2^0(v_1) \Delta D_2(v_1)$.

We partition V_1 in 4 subsets and define for any vertex v_1 a set $S_2(v_1) \subseteq V_2$ as follows

$$\begin{cases} \text{If } v_1 \in D_1 \cap \text{Even}(D_1) & , S_2(v_1) = D_2(v_1) \\ \text{If } v_1 \in D_1 \cap \text{Odd}(D_1) & , S_2(v_1) = C_2^1(v_1) \\ \text{If } v_1 \in V_1 \setminus D_1 \cap \text{Even}(D_1) & , S_2(v_1) = \emptyset \\ \text{If } v_1 \in V_1 \setminus D_1 \cap \text{Odd}(D_1) & , S_2(v_1) = C_2^0(v_1) \end{cases}$$

Consider the set $D_B = \bigcup_{v_1 \in V_1} \{v_1\} \times S_2(v_1)$, $D_B \subseteq B$ and $|D_B| = \sum_{v_1 \in D_1 \cap \text{Even}(D_1)} |D_2(v_1)| + \sum_{v_1 \in D_1 \cap \text{Odd}(D_1)} |C_2^1(v_1)| + \sum_{v_1 \in V_1 \setminus D_1 \cap \text{Odd}(D_1)} |C_2^0(v_1)|$. Therefore $|D_B| = |D_1| = 1 \pmod 2$.

For each $v = (v_1, v_2) \in V \setminus B$, $|\mathcal{N}_G(v) \cap D_B| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + \sum_{u_1 \in \mathcal{N}_{G_1}(v_1)} |S_2(u_1)|$. If $v_1 \in V_1 \setminus D_1$, then $|S_2(v_1)| = 0 \pmod 2$, thus $|\mathcal{N}_G(v) \cap D_B| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + |\mathcal{N}_{G_1}(v_1) \cap D_1| \pmod 2$.

Furthermore, if $v_1 \in \text{Even}(D_1)$, $|\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| = |\mathcal{N}_{G_1}(v_1) \cap D_1| = 0 \pmod 2$ and if $v_1 \in \text{Odd}(D_1)$, $|\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| = |\mathcal{N}_{G_1}(v_1) \cap D_1| = 1 \pmod 2$.

Therefore $|\mathcal{N}_G(v) \cap D_B| = 0 \pmod 2$ which implies that $D_B \cup \text{Odd}(D_B) \subseteq B$.

Furthermore, using Lemma 5, we have $\overline{G_1 * G_2} = \overline{G_1} * \overline{G_2}$. And from corollary 3, as G_1 and G_2 realize $qQSS^*$ protocols $\overline{G_1}$ and $\overline{G_2}$ have the same threshold. Therefore, in $\overline{G_1} * \overline{G_2}$ it exists a set D'_B such that its odd neighborhood in the complementary graph satisfies $\text{Odd}_{\overline{G_1} * \overline{G_2}}(D'_B) \cap V \setminus B = \emptyset$ thus $\text{Odd}_{G_1 * G_2}(D'_B) \cap V \setminus B = V \setminus B$ and D'_B is a valid C_B to define an $((k, n))$ $qQSS^*$ protocol. \square

Let us define $G^{*i} = \underbrace{G * G * \dots * G}_{i \text{ times}}$. If G realizes a $((k, n))$ protocol, we want to find n_i and k_i such that G^{*i} realizes a $((k_i, n_i))$ protocol:

Lemma 7. *Let G be a graph which realizes a $((k, n))$ protocol. Then the graph G^{*i} realizes a $((k_i, n_i))$ protocol where*

$$\begin{cases} n_i = n^i \\ k_i = n^i - (n - k + 1)^i + 1 \end{cases}$$

Proof. By induction: first, we notice that $n_1 = n$ and $k_1 = k$. Then, if we write $G^{*i+1} = G * G^{*i}$, from Lemma 6 $n_{i+1} = n \cdot n_i$ and $k_{i+1} = n \cdot n_i - (n - k + 1)(n_i - k_i + 1) + 1$

One can see that $n_i = n^i$. Now we consider the sequence $u_i = n_i - k_i + 1$. $u_1 = n - k + 1$ and $u_{i+1} = (n - k + 1)u_i$. We deduce that $u_i = (n - k + 1)^i$. Thus, by definition of (u_i) , $k_i = n_i - u_i + 1 = n^i - (n - k + 1)^i + 1$. \square

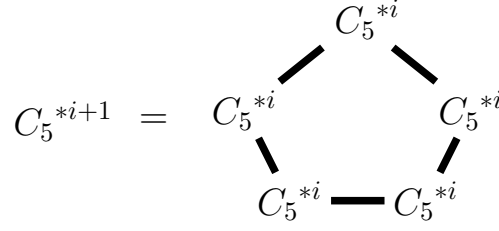


Fig. 2. Decomposition of the graph C_5^{*i+1} .

Theorem 2. For all $i \in \mathbb{N}^*$, the graph C_5^{*i} realizes a $((n, n - n^{\frac{\log(3)}{\log(5)}} + 1))$ protocol (with $n = 5^i$).

Proof. In Lemma 7 with $n = 5$ and $k = 3$ (since the graph C_5 realizes a $((3, 5))$ [13]), we have $n = n_i = 5^i$ and $k_i = 5^i - 3^i + 1 = 5^i - 5^{i \frac{\log(3)}{\log(5)}} + 1 = n - n^{\frac{\log(3)}{\log(5)}} + 1$. \square

4 Lower Bound

By the no-cloning theorem, it is not possible to get two separated copies of the secret starting from only one copy. Thus, if we consider a quantum secret sharing protocol with parameters $((k, n))$ we must have $k > \frac{n}{2}$.

We derive here less trivial lower bounds for our family of protocols.

Definition 2. Let B be a subset of vertices of a graph.

- $D \subseteq B$ is said to be "odd-wise in B " or "B-odd-wise" iff $D \cup \text{Odd}(D) \subseteq B$
- $C \subseteq B$ is said to be "even-wise in B " or "B-even-wise" iff $C \cup \text{Even}(C) \subseteq B$

Lemma 8. Let $G = (V, E)$ be a graph which realizes a $((k, n))$ protocol. Then, for all set B of size k , there exists a set $X \subseteq B$ such that: $|X| \leq \frac{2}{3}(n - k + 1)$ where X is either a B-odd-wise set of size 1 mod 2 or a B-even-wise set.

Proof. First, let $\Gamma_B \in \mathcal{M}_{k, n-k}(\mathbb{F}_2)$ be a cut matrix of G corresponding to the cut $(B, V \setminus B)$. We can see Γ_B as the linear map that maps a set $D \subseteq B$ to its odd neighbourhood in $V \setminus B$: Consequently, any B-odd-wise set D corresponds to a linear combination of the columns of the matrix Γ_B which equals the null vector. Therefore, $\{D \mid D \text{ is odd-wise in } B\} = \text{Ker}(\Gamma_B)$, and $t = \dim(\text{Ker}(\Gamma_B)) = k - \dim(\text{Im}(\Gamma_B)) \geq 2k - n$.

As $|X \Delta Y| = |X| + |Y| \bmod 2$, the sets $\mathcal{D}_1 = \{D \subseteq B, |D| = 1 \bmod 2 \mid D \text{ odd-wise in } B\}$ and $\mathcal{C}_1 = \{C \subseteq B, C \text{ even-wise in } B\}$ are two affine subspaces having the same vector subspace $\mathcal{D}_0 = \{D \subseteq B, |D| = 0 \bmod 2 \mid D \text{ odd-wise in } B\}$.

The dimension of \mathcal{D}_0 is $t - 1$, therefore, by gaussian elimination it exists a set $X_0 \subseteq B$, $|X_0| = t - 1$ such that it exists sets $C_1 \in \mathcal{C}_1$ and $D_1 \in \mathcal{D}_1$ satisfying $X_0 \cap C_1 = X_0 \cap D_1 = \emptyset$. Thus $|C_1 \cup D_1| \leq k - t + 1 \leq n - k + 1$.

Therefore $2|D_1 \cup C_1| = |D_1| + |C_1| + |D_1 \Delta C_1| \leq 2(n - k + 1)$ which implies that one of the three sets has cardinality smaller than $2(n - k + 1)$, as the first set is odd-wise with odd cardinality and the two others are even-wise in B , which concludes the proof. \square

By counting the even-wise and odd-wise sets and their possible completion into q -accessing sets, we get the following lower bound.

Theorem 3. *There exists no graph G that has an $((k, n))$ $qQSS$ protocol with $k < \frac{n}{2} + \frac{n}{157}$.*

Proof. We consider a graph $G = (V, E)$ which realizes a $((k, n))$ secret sharing protocol.

Any set of size $n - k$ is not c -accessing, therefore, any set D , with $|D| = 1 \bmod 2$ satisfies $|D \cup \text{Odd}(D)| \geq n - k + 1$. Consequently, given a set D , with $|D| = 1 \bmod 2$, it exists at most $\binom{n-(n-k+1)}{k-(n-k+1)} = \binom{k-1}{2k-n-1}$ sets B of size k containing $D \cup \text{Odd}(D)$ and such that D is odd-wise in B .

Similarly, any set of size k is c -accessing, for any set C , $|C \cup \text{Even}(C)| \geq n - k + 1$. Therefore, given a set C the number of sets B of size k containing C and such that C is even-wise in B is at most $\binom{k-1}{2k-n-1}$.

With Lemma 8, each set $B \subseteq V$ of size k contains either a B -odd-wise subset D of size odd or a B -even-wise subset C such that $|D| \leq \frac{2}{3}(n - k + 1)$ or $|C| \leq \frac{2}{3}(n - k + 1)$. Thus by counting twice all the sets of cardinality smaller than $\frac{2}{3}(n - k + 1)$ (as a potential odd-wise or even-wise set) we can upper bound the set of possible cuts of size k with $\binom{n}{k} \leq 2 \sum_{i=1}^{\frac{2}{3}(n-k+1)} \binom{n}{i} \binom{k-1}{2k-n-1}$. The previous inequality implies that $k > \frac{n}{2} + \frac{n}{157}$ when $n \rightarrow \infty$. \square

Corollary 4. *There exists no $qQSS$ protocol for $n \geq 79$*

Proof. By Gottesman's characterisation [6] a $qQSS$ protocol has a threshold $((k, 2k - 1))$. Moreover, $k \geq n/2 + n/157$ using the previous lower bound. Therefore $k \leq 159/4$ and the number of players $n = 2k - 1 \geq 79$. \square

References

1. G.R. Blakley, *Safeguarding cryptographic keys*. AFIPS Conference Proceedings. 48 (1979) 313317.
2. D.E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. *Generalized flow and determinism in measurement-based quantum computation*. New Journal of Physics 9, 250, 2007.
3. R. Cleve, D. Gottesman, and H.-K. Lo, *How to Share a Quantum Secret* Phys. Rev. Lett. 83, 648-651 (1999). Also quant-ph/9901025.
4. A. Ekert. *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett. 67, 611, 1991.
5. B. Fortescue and G. Gour. *Reducing the quantum communication cost of quantum secret sharing*. arXiv:1108.5541, 2011.
6. D. Gottesman, *On the Theory of Quantum Secret Sharing*. Phys. Rev. A 61, 042311 (2000) (8 pages). Also quant-ph/9910067.
7. D.M. Greenberger, M.A. Horne, and A. Zeilinger. *Going beyond Bells theorem*. In Bells Theorem, Quantum Theory, and Conceptions of the Universe, pages 6972, 1989
8. M. Hein, J. Eisert, and H. J. Briegel. *Multi-party entanglement in graph states*. Physical Review A, 69, 2004. quant-ph/0307130.
9. M. Hillery, V. Buzek and A. Berthiaume. *Quantum Secret Sharing* Phys. Rev. A 59, p.1829, 1999; e-print quant-ph/9806063.
10. J. Javelle, M. Mhalla and S. Perdrix. *New Protocols and Lower Bound for Quantum Secret Sharing with Graph States* First IQFA workshop, March 2011, and "Codage et Cryptographie" workshop, April 2011.
11. E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix. *Information Flow in Secret Sharing Protocols*. DCM 2009: Elec. Proc. Theor. Comp. Sci. 9, 87 (2009).
12. Adrian Keet, Ben Fortescue, Damian Markham, Barry C. Sanders. *Quantum secret sharing with qudit graph states*. Phys. Rev. A 82, 062315 (2010).
13. D. Markham and B. C. Sanders. *Graph states for quantum secret sharing*. Physical Review A 78, 042309, 2008.
14. A. Nascimento, J. Mueller-Quade, and H. Imai *Improving quantum secret-sharing schemes*. Phys. Rev. A 64 042311, 2001.
15. T. Ogawa, A. Sasaki, M. Imamoto and H. Yamamoto, *Reducing the quantum communication cost of quantum secret sharing*. Phy. Rev. A, 72, 032318, 2005.
16. A. Shamir *How to share a secret* newblock Communications of the ACM 22 (11): 612613, 1979.
17. A. Broadbent, P. R. Chouha, and A. Tapp *The GHZ state in secret sharing and entanglement simulation*. quant-ph/arXiv:0810.0259 , 2008.
18. R. Raussendorf and H. Briegel. *A one-way quantum computer*. PRL 86, 2001.
19. W.K. Wootters and W.H. Zurek. *A Single Quantum Cannot be Cloned*. Nature 299 (1982), pp. 802803.